04-27-00 A

EXPRESS MAIL LABEL NO. EL121365741US
Date of Deposit: April 25, 2000

MDF:rfb 4/25/00

PATENT
Attorney's Ref. No. 245-53436

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Box PATENT APPLICATION
ASSISTANT COMMISSIONER FOR PATENTS
Washington, D.C. 20231

Transmitted herewith for filing is the patent application of:

Inventor(s): Çetin K. Koç, Erkay Savaş

For: CRYPTOGRAPHIC METHODS AND APPARATUS USING WORD-WISE MONTGOMERY MULTIPLICATION

Enclosed are:

☒ 15 pages of specification, 5 pages of claims, an abstract and a Combined Declaration and Power of Attorney (unsigned).
☒ 4 sheet(s) of formal drawings.
☒ Information Disclosure Statement.
☒ Form PTO-1449 and copies of documents listed thereon.

CLAIMS AS FILED

For	Claims Filed	Number Free		Number Extra	Rate	Basic Fee $345.00
Total Claims	21	20	=	1	$9.00	$ 9.00
Independent Claims	8	3	=	5	$39.00	$ 195.00
Multiple Dependent Claim Fee					$130.00	$0.00
TOTAL FILING FEE						$549.00

☒ Please return the enclosed postcard to confirm that the items listed above have been received.

Respectfully submitted,

KLARQUIST SPARKMAN CAMPBELL
LEIGH & WHINSTON, LLP

By _____
Michael D. Jones
Registration No. 41,879

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446
cc: Client
Docketing Secretary

CRYPTOGRAPHIC METHODS AND APPARATUS USING WORD-WISE MONTGOMERY MULTIPLICATION

FIELD OF THE INVENTION

The invention pertains to cryptographic methods and apparatus.

BACKGROUND OF THE INVENTION

Basic arithmetic operations such as addition, multiplication, and inversion performed modulo a prime number p have numerous applications to cryptographic systems. For example, encryption, decryption, or key exchange in Rivest-Shamir-Adelman (RSA), Diffie-Hellman (DH), Digital Signature Standard (DSS), and elliptic curve cryptographic systems all use modular arithmetic operations. These cryptographic systems are described in, for example, W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. 22, pp. 644-654 (1976); B.S. Kaliski Jr., "The Montgomery Inverse and Its Applications," IEEE Trans. Computers, vol. 44, pp. 1064-1065 (1995); J.J. Quisquater and C. Couvreur, "Fast Decipherment Algorithm for RSA Public-Key Cryptosystem," Elect. Lett., vol. 18, pp. 905-907 (1982); and "Digital Signal Standard (DSS)," Fed. Reg., vol. 56, p. 169 (1991).

Modular arithmetic is typically performed on a set Z_p of integers, referred to as a "complete residue" set that is generally defined as, for a selected prime number p, the set of integers 0, 1, 2, 3, . . . , p-1. A complete residue set Z_p is closed with respect to the operations of addition and multiplication, i.e., the sums and products of any elements of the complete residue set Z_p are also elements of the complete residue set Z_p. In addition, each element of Z_p has a multiplicative inverse that is also an element of the complete residue set Z_p.

Multiplication and addition on the complete residue set Z_p are similar to standard multiplication and division, but are performed modulo the prime number p. For example, the modular product $a \cdot b \pmod{p}$ is obtained by calculating the product $a \cdot b$, and then dividing by p one or more times to obtain a remainder that is an element of the complete residue set Z_p. As a specific example, the product of integers $a = 5$, $b = 6$ computed modulo-p for $p = 11$, is $a \cdot b = 5 \cdot 6 \pmod{11} = 30 \pmod{11} = 8$. The modular inverse a^{-1} of an element a of Z_p is the element of Z_p such that $a \cdot a^{-1} = 1 \pmod{p}$. As a specific example, for $a = 6$, $p = 11$, $a^{-1} = 2$ because $6 \cdot 2 \pmod{11} = 1$.

Many important cryptographic systems require a substantial number of modular multiplications and computations of modular multiplicative inverses. As used herein, "inverse" and "inversion" refer to inverse operations with respect to multiplication. Fast, efficient multiplication and inversion methods are needed to carry out such calculations. One such method is the Montgomery method, described in P. L. Montgomery, "Modular Multiplication Without Trial Division," Math. of Computation, vol. 44, pp. 519-521 (1985), in which integers a that are elements of the complete residue set Z_p are transformed into corresponding integers A referred to as "M-residues" (also elements of Z_p) according to the transformation $A = a\ 2^n \pmod{p}$, wherein the integer n is selected so that $2^{n-1} \leq p < 2^n$. A Montgomery product MPROD of two M-residues A, B of respective integers a, b is defined as:

$$C = \text{MPROD}(A,B) \equiv A\ B\ 2^{-n} \pmod{p},$$

and is the M-residue of the modulo-p product $c = a\ b$. The product c can be obtained from the M-residue product C as:

$$c = C\ 2^{-n} \pmod{p}.$$

Calculation of the modular product $c = ab$ using the Montgomery product of the M-residues A, B of a, b is typically faster than direct modular multiplication of a, b because the Montgomery product requires only

divisions by two that are easily implemented as bit-shifting operations on a binary number-based digital computer.

Modular exponentiation and modular multiplicative inversion are other common operations in cryptographic systems. In many cryptographic applications, both an M-residue of c, i.e., $C = c\ 2^n \pmod{p}$ and a quantity referred to as a "Montgomery inverse" are needed. A particular Montgomery inverse $c^{-1}2^n \pmod{p}$ and a method for its computation are discussed in B.S. Kaliski Jr., "The Montgomery Inverse and Its Applications," cited above. This Montgomery inverse is referred to as a "Kaliski inverse" KINV() herein. With reference to Table 1, the Montgomery inverse KINV(a) is obtained by first calculating an intermediate value $a^{-1}\ 2^k \pmod{p}$ in a phase I, and then correcting this intermediate value to obtain the Montgomery inverse KINV(a) $= a^{-1}\ 2^n \pmod{p}$ in a phase II.

Table 1. Pseudocode for determination of a Montgomery inverse

```
PHASE I
input  a, p,  wherein 1 ≤ a ≤ p-1
u = p; v = a; r = 0; s = 1
k = 0
while (v > 0)
      if u is even then u = u/2, s = 2s
      else if v is even then v = v/2, r = 2r
      else if u > v then u = (u-v)/2, r = r+s, s = 2s
      else if v ≥ u then v = (v-u)/2, s = s+r, r = 2r
      k = k+1
if r ≥ p then r = r-p
return r = a^-1 2^k (mod p), and k, wherein n ≤ k ≤ 2n

PHASE II
Input r, k , p (from PHASE I)
for I = 0 to I = k-n, do
      if r is even then r = r/2
      else then r = (r+p)/2
x = r
return x, wherein 1 ≤ x ≤ p − 1 and x = a^-1 2^n (mod p)
```

Unfortunately, obtaining a Montgomery product MPROD or a Montgomery inverse KINV() using the Montgomery product typically requires transforming numbers expressed as elements of the complete residue set Z_p to and from their respective M-residues. These transformations make such calculations slow and expensive. In addition, because cryptographic systems often require many modular multiplications, the speed and efficiency of such calculations can limit the utility of a cryptographic system. Hence, improved methods and apparatus are needed for obtaining Montgomery products and Montgomery inverses.

SUMMARY OF THE INVENTION

According to a first aspect of the invention, methods are provided for transforming a message represented as an element of a complete residue set modulo a prime number p into a Montgomery residue of a multiplicative inverse. The methods include selecting a Montgomery radix $R = 2^m$, wherein m is an integer multiple of a wordsize and m is greater than a bit-length of the prime number p. An "almost Montgomery inverse procedure" is used to determine quantities (r, k), wherein r is an intermediate value and k is an integer. If k is greater than m, then a multiplicative inverse is obtained as a Montgomery product of r and 2^{2m-k}. If k is less than or equal to m, then r is assigned a new value that is equal to a Montgomery product of r and a square of the Montgomery radix R modulo the prime number p, and k is assigned a value $k = k + m$. The multiplicative inverse is then obtained as a Montgomery product of r and 2^{2m-k}. In representative embodiments, a stored value of R^2 mod p is retrieved and the method is implemented as instructions contained on a computer-readable medium.

According to another aspect of the invention, methods are provided for obtaining a classical inverse of a message, represented as a series of binary digits, that is an element of a residue set modulo a prime number p.

The methods include obtaining values (r,k) using almost Montgomery inverse procedure, wherein a Montgomery radix $R = 2^m$, and m is an integer multiple of a wordsize and is greater than a bit-length of the prime number p. If k is less than or equal to m, then a classical inverse is calculated as a Montgomery product of r and 2^{m-k}. If k is greater than m, then r is assigned a value equal to a Montgomery product of r and 1, and k is assigned a value of $k - m$. The classical inverse is then calculated as a Montgomery product of r and 2^{m-k}.

According to another aspect of the invention, cryptographic systems are provided that include modules for performing such methods. The systems include hardware, software, or a combination thereof. Computer-readable media containing instructions for these methods are also provided.

The cryptographic methods can include representing a message as a series of binary digits, the series being divisible into an integer number m of words. A prime number p is selected and an intermediate product r and an integer k are obtained using an almost Montgomery inverse procedure, wherein a Montgomery radix $R = 2^m$, and m is greater than a bit-length of the prime number p. If k is greater than m, then a multiplicative inverse is computed as a Montgomery product of r and 2^{2m-k}. If $k \leq m$, then r is assigned a value equal to a Montgomery product of r and R^2, and k is assigned a value of $k + m$. A multiplicative inverse is then computed as a Montgomery product of r and 2^{2m-k}. The methods can further comprise retrieving a stored value of $R^2 \bmod p$.

According to another aspect of the invention, methods are provided for computing a classical inverse of a message a that is represented as a sequence of binary digits. The methods include obtaining $r = a^{-1}2^m \pmod p$, wherein m is an integer that is an integer multiple of a wordsize, a Montgomery radix $R = 2^m$, and p is a prime number. The multiplicative inverse is then calculated as a Montgomery product of r and 1.

In additional methods, a Montgomery product r of a message a with a square of a Montgomery radix $R = 2^m$ is obtained, and an inverse KINV(r) is computed to obtain a classical inverse of a.

Methods of computing a multiplicative inverse of an M-residue $A = a2^m \bmod p$, wherein p is a prime number, can include computing an intermediate product r and an integer k using an almost Montgomery inverse procedure. If k is greater than m, then the intermediate product r is assigned the value of the Montgomery product of r and R^2, and a multiplicative inverse is obtained as a Montgomery product of r and 2^{2m-k} using a Montgomery radix $R = 2^m$. If k is less than or equal to m, then r is assigned a value equal to a Montgomery product of r and R^2, and k is assigned a value of $k + m$. Montgomery products with R^2 and 2^{2m-k} then are obtained to produce the multiplicative inverse.

Computer-readable media containing instructions for performing these methods also are provided as well as cryptographic systems that include hardware, software, or a combination thereof for performing these methods.

Cryptographic methods for processing a series of binary digits divided into an integer number m of words can include executing an almost Montgomery inverse procedure to obtain an intermediate value r and an integer k. The intermediate value r is then transformed by determining a Montgomery product of r with respect to a Montgomery radix R^2 2^m and a prime number p.

In additional embodiments, cryptographic methods include selecting a Montgomery radix based on a number of words in a message and performing a Montgomery multiplication to transform the message.

These and other features and advantages of the invention are described below with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a method for computing a Montgomery residue of a classical inverse of an element of a complete residue set.

FIG. 2 is a block diagram of a method for computing a classical inverse of an element of a complete residue set.

FIG. 3 is a block diagram of a method for computing an alternative Montgomery residue.

FIG. 4 is a schematic diagram of a smartcard that includes a cryptographic processor module.

DETAILED DESCRIPTION

As used herein, lower-case letters represent elements of a complete residue set Z_p, upper-case letters represent corresponding M-residues, and p is a prime number. Unless stated otherwise, modular multiplications are carried out modulo-p. An M-residue of an element a of Z_p is defined as $A = a\,R \bmod p$, wherein $2^{n-1} < p < 2^n$, n is an integer, and $R = 2^n$ is a Montgomery radix. Although M-residues of the elements of the complete residue set are also elements of Z_p, for convenience herein, untransformed elements of Z_p are referred to as "C-residues," while values obtained as $A = a\,R \bmod p$ are referred to as "M-residues."

A Montgomery product of M-residues A,B is defined as:

$$C = \mathrm{MPROD}(A,B) = A\,B\,R^{-1} \pmod p,$$

wherein C is an M-residue of the product $a\,b \pmod p$ and $R = 2^n$ is a Montgomery radix, wherein $n \leq p$. A multiplicative inverse KINV(), as described in the Kaliski reference cited above, is defined as $\mathrm{KINV}(a) = a^{-1}R \bmod p$, and a Montgomery product of a and the Kaliski inverse KINV(a) is:

$$\mathrm{MPROD}(a, \mathrm{KINV}(a)) = a\,a^{-1}\,2^n\,2^{-n} \pmod p = 1 \pmod p.$$

This product is the M-residue of 2^{-n}.

With reference to Table 1, above, the Kaliski inverse KINV(a) of a can be obtained by first calculating an intermediate value $a^{-1}\ 2^k \pmod p$ in a phase I, and then correcting this intermediate value to obtain the inverse KINV(a) $= a^{-1}\ 2^n \pmod p$ in a phase II. For convenience, the phase I output of the procedure of Table 1 is referred to herein as an "almost" Montgomery inverse ("AMI") and is defined as:

$$(r, k) = \text{AMI}(a) = a^{-1}\ 2^k \pmod p,$$

wherein r is referred to as an "intermediate value" of a multiplicative inverse, and 2^k is an intermediate radix. Because the phase I output includes r and k, the value of k is included as a result of the almost Montgomery inverse AMI(). The procedure of Phase I is referred to as an "AMI procedure."

Many cryptographic operations using Montgomery products involve both a C-residue (or M-residue) and an inverse thereof. For example, a "classical" inverse a^{-1} of a is defined such that $a\ a^{-1} = 1 \bmod p$. Additional inverses and methods for obtaining inverses are described below. For clarity, the classical inverse a^{-1} is also written as CINV(a).

To permit increased computational efficiency, a modified radix $R_m = 2^m$ is substituted for the conventional Montgomery radix $R = 2^n$, wherein m is an integer multiple of a number of bits w in a word ("word size"). The word size typically depends on the computer or other computational hardware used for encryption or decryption. Any value of m greater than or equal to a number of bits in the modulus p is suitable, but for increased efficiency, the smallest multiple of w that is greater than or equal to p is preferable. A word-length radix permits word-by-word ("word-wise") multiplications that are generally more efficient than bit-wise multiplications.

With reference to Table 2, a function MINV(a) first calculates an inverse a^{-1} of an element a of Z_p and then converts a^{-1} to a corresponding M-residue. The AMI procedure is used first to obtain (r,k) from the function AMI(a), followed by one or two word-wise Montgomery product operations

(i.e., multiplications by 2^m or a power thereof) using the modified Montgomery radix $R_m = 2^m$. The method of Table 2 uses at most two Montgomery product operations after computing the AMI(*a*), and is therefore faster and more efficient than prior art methods that require up to three Montgomery product operations.

Table 2. Pseudocode for obtaining an M-residue of a classical inverse

```
FUNCTION MINV(a), finds inverse, then M-residue
input a, p, n, m
(r,k) = AMI(a), wherein r = a^-1 2^k (mod p) and n ≤ k ≤ m+n
if n ≤ k ≤ m, then
      r = MPROD(r, R^2) = (a^-1 2^k)(2^2m)(2^-m) (mod p)
      = a^-1 2^m = k (mod p)
      k = k + m > m
end if
r = MPROD(r, 2^2m-k) = a^-1 2^k 2^2m-k 2^-m (mod p)  = a^-1 2^m (mod p)
output r = a^-1 2^m (mod p)
```

The procedure of Table 2 is illustrated in FIG. 1. A module 100 receives the element *a* (and parameters *n*, *m*, and *p*) as an input in an input block 101. Typically the parameters *n*, *m*, and *p* are stored and need not be re-entered as new elements. The element a and the remaining parameters are used by a processing block 103 that computes an intermediate value *r* and an integer *k* using an almost Montgomery inverse procedure. The values (*r*,*k*) are communicated to a decision block 105. If $n \leq k \leq m$, then the decision block 105 directs the intermediate value *r* to a Montgomery-product block 107 to compute a Montgomery-product of the intermediate value of *r* and R^2. The Montgomery-product block 107 also assigns *k* a value of $k + m$. Typically, a storage block 111 stores a value or R^2 mod *p* for retrieval by the Montgomery-product block 107. After the calculations performed in the Montgomery-product block 107 are complete, or if such calculations were unnecessary, then a Montgomery-product block 109

computes a Montgomery product of the intermediate value r with 2^{m-k}. After completion of the Montgomery-product block 109, an output block 115 returns a final value of r that is the M-residue of the classical inverse.

The classical inverse a^{-1} = CINV(a) also can be obtained using the AMI procedure and the modified Montgomery radix R_m. With reference to Table 3, the classical inverse a^{-1} = CINV(a) is calculated by evaluating the function AMI(a), followed by at most two MPROD operations (Montgomery products) with 1 and 2^{m-k}. Word-wise computation of the classical inverse using the function AMI(a) and the modified Montgomery radix R_m is efficient.

Table 3. Pseudocode for determining a classical inverse CINV(a)

```
FUNCTION CINV(a)
input a, p, n , m, wherein 1 ≤ a ≤ 2^(m-1)
(r,k) = AMI(a) = (a^-1 2^k (mod p), k), wherein n ≤ k ≤ m+n
if k > m, then
        r = MPROD (r,1) = (a^-1 2^k) (2^-m) = a^-1 2^(k-m) (mod p)
        k = k-m < m
r = MPROD (r, 2^(m-k)) = (a^-1) 2^k 2^(m-k) 2^-m = a^-1 (mod p)
return r
```

The procedure of Table 3 is illustrated in FIG. 2. A module 200 receives the element a and values of p, m, and n as inputs in an input block 201. As noted above, the values p, m, and n can be retrieved from storage. A processing block 203 computes an intermediate value r and an integer k using an almost Montgomery inverse procedure. The values (r,k) are communicated to a decision block 205. If $k \geq m$, then a Montgomery-product block 207 computes a Montgomery product of r with 1 and decrements k by m. The intermediate value r from the Montgomery-product block 207 ($k \geq m$) or the decision block 205 ($k < m$) is directed to a Montgomery-product block 209 that computes a Montgomery product of the intermediate value r with 2^{m-k}. After completion of the calculation in the

Montgomery-product block 209, an output block 215 returns a final value of r that is the classical inverse of the element a.

As noted above, the Montgomery product of the Montgomery inverse KINV(a) and a is 1 (mod p). Unfortunately, 1 (mod p) is the M-residue of 2^m and is not the M-residue of the product $a\,a^{-1}$. The product of a and a^{-1} preferably corresponds to the M-residue of $a\,a^{-1}$, i.e., 2^m (mod p). Accordingly, an "alternative Montgomery inverse" NINV(A) is defined as:

$$\text{NINV}(A) = \text{NINV}(a2^m) = (a2^m)^{-1}\,2^{2m} \pmod p = a^{-1}\,2^m \pmod p.$$

As defined herein, NINV(A) is a function of the M-residue A. A Montgomery product MPROD of an M-residue A with the alternative inverse NINV(A) is:

$$\text{MPROD}(A, \text{NINV}(A)) = (a2^m)\,(a^{-1}\,2^m)\,2^{-m} = 2^m \pmod p.$$

Thus, the product 2^m mod p is the M-residue corresponding to the product $a\,a^{-1}$ with respect to the modified radix R_m.

The alternative Montgomery inverse NINV(A) can be obtained by several methods. In one method, the alternative Montgomery inverse NINV(A) is computed by first calculating KINV(A) = KINV($a2^m$) = $(a2^m)^{-1}\,2^m = a^{-1} \pmod p$, and then calculating a Montgomery product MPROD of KINV(A) with $R^2 = 2^{2m}$:

$$\text{MPROD}\,(\text{KINV}(A), R^2) = \text{MPROD}\,(a^{-1}, R^2) = a^{-1}\,2^{2m}\,2^{-m} = a^{-1}2^m \pmod p.$$

In a second method, the alternative Montgomery inverse NINV(A) is computed by first calculating a Montgomery product of $A = a2^m$ with the number 1:

$$\text{MPROD}(a2^m, 1) = (a2^m)\,(1)\,(2^{-m}) = a \pmod p,$$

and then calculating a Kaliski inverse KINV(a):

$$\text{KINV}(a) = a^{-1}2^m \pmod p.$$

In a third method illustrated in Table 4, NINV(a) is calculated by first calculating the almost Montgomery inverse AMI(A) to produce values (r, k).

Then, two or three Montgomery products of r are calculated (with R^2 and 2^{2m-k}), depending on the value of k returned by AMI($a2^m$). The method of Table 4 uses at most three MPROD operations in addition to the AMI procedure.

Table 4. Pseudocode for determining an alternative inverse NINV(A)

```
FUNCTION NINV(A)
Input A = a2^m (mod p), p, n, m
(r,k) = AMI(a2^m (mod p)) = (a^-1 2^-m 2^k (mod p),k), wherein n ≤ k ≤ m+n
      if n ≤ k ≤ m then
      r = MPROD (r, R^2) = (a^-1 2^-m 2^k)2^2m 2^-m = a^-1 2^k(mod p)
      k = k+m > m
end if
r = MPROD (r, R^2) = (a^-1 2^-m 2^k)2^2m 2^-m = a^-1 2^k(mod p)
r = MPROD (r, 2^2m-k) = (a^-1 2^k) (2^2m-k) (2^-m) = a^-1 2^m(mod p)
return r = a^-1 2^m(mod p)
```

The procedure of Table 4 is illustrated in FIG. 3. A module 300 receives the element A in an input block 301. The element A is communicated to a processing block 303 that computes an intermediate value r and an integer k using an almost Montgomery inverse method. The values (r,k) are then communicated to a decision block 305. If $n \le k \le m$, then a Montgomery-product block 307 computes a Montgomery product of the intermediate value r with R^2. For convenience, a value of R^2 mod p can be retrieved from a storage block 311. After completion of the calculation in the Montgomery-product block 307 or after exiting the decision block 305, Montgomery-product blocks 309, 313 compute Montgomery products with R^2 and 2^{2m-k}, respectively, wherein each of the Montgomery-product blocks 309, 313 assigns the intermediate value r a new value equal to a result of the corresponding Montgomery product operation. An output block 315 returns a final value of r that is equal to the alternative inverse NINV(A).

As described above, these methods for determining NINV(A) use the modified Montgomery radix R_m and can use word-wise multiplication. Because the determination of the alternative Montgomery inverse NINV(A) calculations can use a pre-computed value of $R^2 \pmod{p}$, computation of NINV(A) can be fast and efficient.

C-language modules for implementing several of the methods described above are provided in Appendix A.

A total computation time for NINV(), according to the invention, can be significantly faster than the bit-wise calculation of KINV(). Furthermore, the alternative inverse is an inverse of a with respect to the Montgomery product operation, i.e., MPROD(a, NINV(a)) = $2^m \pmod{p}$, which is the M-residue of $a\ a^{-1}$.

These improved methods of Montgomery multiplication and the determination of inverses with respect to Montgomery multiplication have application to encryption and decryption systems used to provide computer data security and secure transmission of data, including financial data and text, over insecure communication channels such as the Internet and wireless systems such as cellular telephone systems. In addition, systems for user authentication use Montgomery multiplication methods. Such systems are important in many applications, but especially in financial transactions in which it is critical to determine that a particular user has authorized a particular purchase or fund transfer. These systems represent text messages, numerical data (such as financial data), or user access information (e.g., passwords, public keys, private keys, authentication codes, or other encryption/decryption parameters) as words comprising a series of binary bits. These words are referred to herein as "messages" for convenience. These messages can be manipulated using the above methods to facilitate encryption and decryption.

Cryptographic systems and apparatus can include modules or software components that perform necessary arithmetic operations such as the Montgomery inversions and other operations described above. Such modules can include dedicated (application-specific) integrated circuits or other processing hardware. Alternatively, the Montgomery operations can be implemented in software that is executed on a general purpose microprocessor. For example, as shown in FIG. 4, a smartcard 401 includes a cryptographic module 407, typically implemented as a combination of hardware and software and a user identifier 411. The cryptographic protocols used by the smartcard 401 are implemented by the cryptographic module 407 that is in communication with a processor module 405 that implements various mathematical operations associated with encryption and decryption. The processor module 405 includes hardware, software, or a combination of hardware and software for determining Montgomery inverses and classical inverses of sequences of binary digits as well as Montgomery multiplication.

One specific example of a cryptographic system includes an encryption processor that receives unencrypted data or text ("plaintext"), typically as a computer file, and produces encrypted data or text ("ciphertext"). In a representative application to elliptical curve cryptography, a quantity eP is to be determined, wherein e is an integer and P is a point on an elliptic curve defined over the finite field GF(p). This determination requires addition of points P, Q, i.e., $P+Q$, and a doubling operation $P + P = 2P$. Such point operations typically require several modular additions and multiplications, and an inversion. An inversion operation is used to compute a quantity $\lambda = (y_2 - y_1)(x_2 - x_1)^{-1}$, wherein points P and Q are specified with coordinates (x_1, y_1) and (x_2, y_2). Using NINV(), this computation can be performed as follows:

$NINV((x_2 - x_1)\ 2^m)) = (x_2 - x_1)^{-1}\ 2^m \pmod{p}$

$MPROD((y_2 - y_1)\ 2^m, (x_2 - x_1)^{-1}\ 2^m) = \lambda 2^m$,

as required. Because this result is an M-residue, subsequent computations can be performed without transformation of a C-residue to an M-residue. As a result, not only are the wordwise procedures faster than conventional procedures, the wordwise procedures can omit C- to M-residue transformations, further increasing computational speed.

As another example, in an RSA encryption/decryption system, prime numbers p, q are selected and a product $n = pq$ computed. In addition, a quantity $f(n) = (p - 1)(q - 1)$ is calculated, and another integer e is chosen such that the greatest common denominator of e and $f(n)$ is 1. Finally, a quantity $d = e^{-1} \bmod (f(n))$ is calculated.

Typically, the values of e, n are publicly known and provide a so-called public key. The values of d, p, q are kept secret. A plaintext T is encrypted to produce a ciphertext U as $U = T^e \bmod n$, using the public key. The ciphertext U is decrypted to recover the plaintext as $T = U^d \bmod n$. These computations are conveniently performed using Montgomery multiplication and Montgomery inverses to decrease the complexity of the encryption and decryption operations. In particular, determination of the parameter d is facilitated using the Montgomery inversion methods described herein.

While the invention is described with reference to several examples, it will be understood, by those skilled in the art to which the invention pertains, that the examples may be modified without departing from the spirit and scope of the invention that is to be limited only by the appended claims.

We claim:

1. A method for transforming a message represented as an element of a complete residue set modulo a prime number p into a Montgomery residue of a multiplicative inverse, the method comprising:

selecting a Montgomery radix $R = 2^m$, wherein m is an integer multiple of a wordsize, and m is greater than a bit-length of the prime number p;

determining (r, k) from an almost Montgomery inverse function;

if k is less than m, then assigning r a value obtained as a Montgomery product of r and R^2 mod p, and assigning k a value $k = k + m$; and

obtaining the multiplicative inverse as a Montgomery product of r and 2^{2m-k}.

2. The method of claim 1, further comprising retrieving a stored value of R^2 mod p.

3. A computer-readable medium containing instructions for performing the method of claim 2.

4. A computer-readable medium containing instructions for performing the method of claim 1.

5. A cryptographic system for encryption and decryption, the system comprising a module for transforming a message as recited in claim 1.

6. The method of claim 1, wherein the message is a ciphertext.

7. A method for obtaining a classical inverse of a message, represented as a series of binary digits, that is an element of a residue set modulo a prime number p, the method comprising:

obtaining values (r,k) by calculating an almost Montgomery inverse function of the representation of the message using a Montgomery radix $R = 2^m$, wherein m is an integer multiple of a wordsize and is greater than a bit-length of the prime number p;

if k is greater than m, then assigning r a value equal to a Montgomery product of r and 1, and assigning k a value of $k - m$; and

calculating the classical inverse as a Montgomery product of r and 2^{m-k}.

8. A cryptographic system, comprising an encryption/decryption module that performs the method of claim 7.

9. The cryptographic system of claim 8, further comprising at least one integrated circuit.

10. A computer-readable medium, comprising instructions for performing the method of claim 7.

11. A cryptographic method, comprising:

representing a message as a series of binary digits, the series being divisible into an integer number m of words;

selecting a prime number p;

obtaining an intermediate product r and an integer k using an almost Montgomery inverse procedure, wherein a Montgomery radix $R = 2^m$, and m is greater than a bit-length of the prime number p;

if $k < m$, then assigning r a value obtained as a Montgomery product of r and R^2 mod p, and assigning k a value of $k + m$;

assigning r a value obtained as a Montgomery product of r' and R^2 mod p; and

obtaining a multiplicative inverse as a Montgomery product of r and 2^{2m-k}.

12. The method of claim 11, further comprising retrieving a stored value of R^2 mod p.

13. A computer-readable medium containing instructions for performing the method of claim 12.

14. A method for computing a classical inverse of a message a, the method comprising:

(a) selecting an integer m that is greater than a bit-length of the message a, and selecting a Montgomery radix $R = 2^m$;

(b) selecting a prime number p;

(c) representing the message a as a series of binary digits, the series being divided into m words;

(d) obtaining a value $r = a^{-1}2^m \pmod{p}$;

(e) obtaining the classical inverse as a Montgomery product of r and 1.

15. A method for computing a classical inverse of a message a, the method comprising:

(a) selecting an integer m that is greater than a bit-length of the message a, and selecting a Montgomery radix $R = 2^m$;

(b) selecting a prime number p;

(c) representing the message a as a series of binary digits, the series being divided into m words;

(d) obtaining a value r as a Montgomery product of the message a and R^2 mod p; and

(e) obtaining the classical inverse as a Kaliski inverse of r.

16. A method for computing a multiplicative inverse of an M-residue $A = a2^m \bmod p$, wherein p is a prime number, m is an integer, and a Montgomery radix $R = 2^m$, the method comprising: computing an intermediate product r and an integer k using an almost Montgomery inverse procedure;

assigning an intermediate product r' the value of a Montgomery product of r and R^2; and

obtaining the multiplicative inverse as a Montgomery product of r' and 2^{2m-k}.

17. The method of claim 16, further comprising:

determining if the integer k is greater than or equal to m; and

if the integer k is k is greater than or equal to m, assigning the intermediate product r' the value of a Montgomery product of r and R^2 and assigning k a value of $k + m$ prior to obtaining the step of obtaining the multiplicative inverse.

18. The method of claim 16, further comprising retrieving a value of R^2 mod p.

19. A computer-readable medium containing instructions for performing the method of claim 18.

20. A cryptographic method for processing a series of binary digits divided into an integer number m of words, the method comprising:

selecting a Montgomery radix $R = 2^m$ and a prime number p;

executing an almost Montgomery inverse procedure to obtain an intermediate value r and an integer k; and

obtaining a Montgomery product of r.

21. A cryptographic method, comprising:

dividing a message into at least two words;

selecting a Montgomery radix based on a number of words in the message; and

performing a Montgomery multiplication to transform the message.

CRYPTOGRAPHIC METHODS AND APPARATUS USING WORD-WISE MONTGOMERY MULTIPLICATION

ABSTRACT

Cryptographic methods and apparatus are provided for determination of multiplicative inverses. A Montgomery radix is selected based on a wordsize, permitting word-wise Montgomery multiplication. Using word-wise Montgomery multiplication, methods and apparatus determine various multiplicative inverses with reduced computation time.

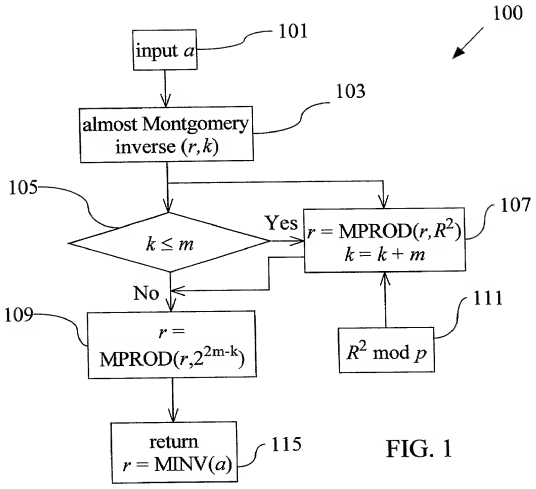
100
input a
101
almost Montgomery inverse (r,k)
103
105
$k \le m$
Yes
$r = \text{MPROD}(r, R^2)$
$k = k + m$
107
No
109
$r = \text{MPROD}(r, 2^{2m-k})$
$R^2 \bmod p$
111
return $r = \text{MINV}(a)$
115

FIG. 1

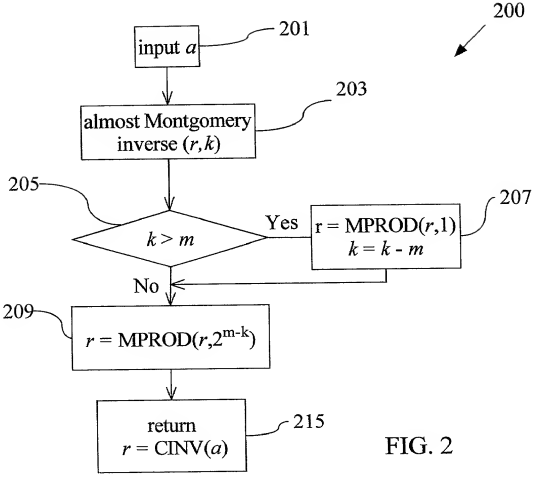
200
input a
201
almost Montgomery inverse (r,k)
203
205
$k > m$
Yes
r = MPROD(r,1)
$k = k - m$
207
No
209
r = MPROD(r,2^{m-k})
return
r = CINV(a)
215

FIG. 2

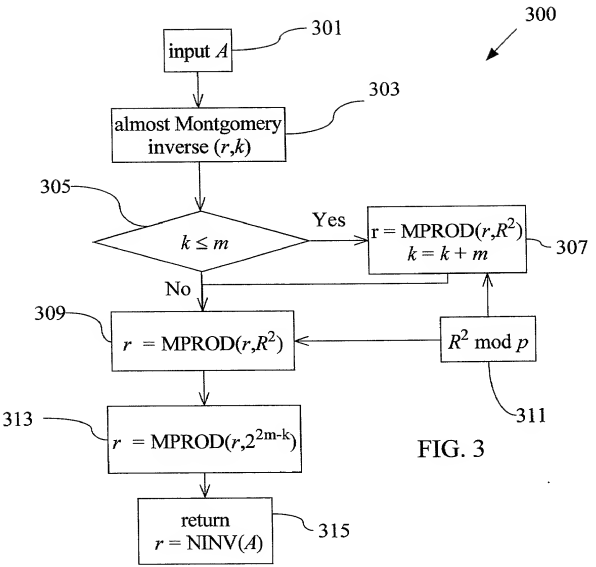
300
input A
301
almost Montgomery inverse (r,k)
303
305
$k \leq m$
Yes
r = MPROD(r,R^2)
$k = k + m$
307
No
309
r = MPROD(r,R^2)
R^2 mod p
311
313
r = MPROD(r,2^{2m-k})
return
r = NINV(A)
315

FIG. 3

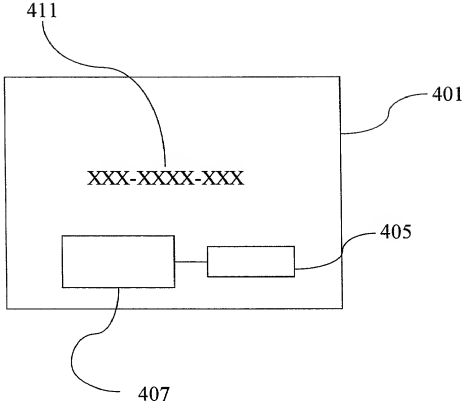

FIG. 4

COMBINED DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled CRYPTOGRAPHIC METHODS AND APPARATUS USING WORD-WISE MONTGOMERY MULTIPLICATION, the specification of which

[X] is attached hereto.

[ ] was filed on _____ as Application No. _____.

[ ] was described and claimed in PCT International Application No. _____, filed on _____, and as amended under PCT Article 19 on _____ (if applicable).

[ ] and was amended on _____ (if applicable).

[ ] with amendments through _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56. If this is a continuation-in-part application filed under the conditions specified in 35 U.S.C. § 120 which discloses and claims subject matter in addition to that disclosed in the prior copending application, I further acknowledge the duty to disclose material information as defined in 37 C.F.R. § 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) of any foreign application(s) for patent or inventor's certificate or of any PCT International application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT International application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	[ ] Yes	[ ] No

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below:

Application Number	Filing Date
60/193,676	March 31, 2000

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) or

§ 365(c) of any PCT International application(s) designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT International filing date of this application:

(Application No.)	(Filing Date)	(Status: patented, Pending, abandoned)

The undersigned hereby authorizes the U.S. attorney or agent named herein to accept and follow instructions from _____ as to any action to be taken in the Patent and Trademark Office regarding this application without direct communication between the U.S. attorney or agent and the undersigned. In the event of a change in the persons from whom instructions may be taken, the U.S. attorney or agent named herein will be so notified by the undersigned.

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application, to file a corresponding international application, and to transact all business in the Patent and Trademark Office connected therewith:

Name	Reg. No.	Name	Reg. No.
BECKER, Mark L.	31,325	NOONAN, William D.	30,878
CALDWELL, Lisa M.	41,653	PETERSEN, David P.	28,106
DeGRANDIS, Paula A.	43,581	POLLEY, Richard J.	28,107
GEORGE, Samuel E.	44,119	SCOTTI, Robert F.	39,830
GIRARD, Michael P.	38,467	SIEGEL, Susan Alpert	43,121
HARDING, Tanya M.	42,630	SLATER, Stacey C.	36,011
JAKUBEK, Joseph T.	34,190	STEPHENS Jr., Donald L.	34,022
JOHNSON, Michelle L.	36,352	STUART, John W.	24,540
JONES, Michael D.	41,879	VANDENBERG, John D.	31,312
KLARQUIST, Kenneth S.	16,445	WHINSTON, Arthur L.	19,155
KLITZKE II, Ramon A.	30,188	WIGHT, Stephen A.	37,759
LEIGH, James S.	20,434	WINN, Garth A.	33,220
MAURER, Gregory L.	43,781		

Address all telephone calls to Michael D. Jones at telephone number (503) 226-7391.

Address all correspondence to:

KLARQUIST SPARKMAN CAMPBELL
LEIGH & WHINSTON, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204-2988

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

MDJ:rfb 4/25/00 245-53435

Full Name of Sole or first Inventor: Çetin K. Koç

Inventor's Signature _____ Date _____

Residence: Corvallis, Oregon

Citizenship:

Post Office Address: 1250 NW 17th Street
Corvallis, Oregon 97330

Full Name of Second Joint Inventor, if any: Erkay Savaş

Inventor's Signature _____ Date _____

Residence: Corvallis, Oregon

Citizenship:

Post Office Address: 1237 NW 23rd Street
Corvallis, Oregon 97330